Office Action Summary	Application No.	Applicant(s)	
	10/809,267	CAMENISCH ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 2 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2008*.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☒ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7,14 and 18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☒ Claim(s) *1-4,7,14 and 18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed July 23, 2008. Claims 1, 7 and 14, and 18 have been amended; Claims 5, 6, 8-13 and 15-17 have been cancelled. Claims 1-4, 7, 14 and 18 are pending and have been considered below.

Claim Rejections - 35 USC § 112

2. Claims 1, 5, 7, 9, 10, 12, 14, 16 and 18 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The rejection has been withdrawn in light of the amendment to claims 1, 7, 14 and 18 and the cancellation of the claims 5, 10, and 12.

Claim Rejections - 35 USC § 101

3. Claims 9, 10 and 12 were rejected as been drawn to a computer program per se. The rejection has been withdrawn in light of the cancellation to the claims.

Specification

4. The abstract of the disclosure is objected to because The abstract contains Fig.2, the title of the invention and numbering of the lines. Correction is required. See MPEP § 608.01(b).

Claim Objections

5. Claims 1, 2, 3, 4, 7, 14 and 18 objected to because of the following informalities:

Regarding Claim 1:

Line 16 recites the limitation of "the secret key"; the examiner suggests "the secret random key".

Regarding Claim 2:

Line 1 recites the limitation of "a random secret key", the examiner suggest, "the random secret key".

Regarding Claim 3:

Line 1 recites the limitation of "a random secret key", the examiner suggest "the random secret key".

Regarding Claim 4:

Line 1 recites the limitation of "a random secret key", the examiner suggests, "the random secret key".

Regarding claim 7:

Line 7 recites the limitation of "the random secret key", the examiner suggests, "a random secret key".

Line 8 recites the limitation of "said secret key", the examiner suggests, "said random secret key".

Line 12 recites the limitation of "to be sent", the examiner suggests, "to be received".

Line 12 recites the limitation of "to a second", the examiner suggests, "from the first".

Regarding Claim 14:

Line 18 recites the limitation of "the secret key", the examiner suggests, "the random secret key".

Regarding Claim 18:

Line 13 recites the limitation of "to be sent", the examiner suggests, "to be received".

Line 13 recites the limitation of "to a second", the examiner suggests, "from the first".

Appropriate correction is required.

Allowable Subject Matter

6. Claims 1-4, 7, 14 and 18 would be allowable if rewritten or amended to overcome the objections set forth in this Office action.

Examiner's Statement of Reasons for Allowance

6. Prior art references were found which disclosed a cryptographic key generation and safekeeping process whereby source code is loaded on a secure computer system with a "master-key" and "Locking-key" compiled from the source code and then stored on disks (Abstract, Col. 12, lines 43-46). Moreover, a public exponent e" which is derived from an RSA modulus N and private exponent d. (Col. 9, lines 19-28) Brennan et al (US 5,675,649), and Arditti et al (US 6,125445) which spoke to determining some

sort of interval based on a parameter "m" from which an exponent value "a" that a "claimant" entity can use and an exponent "[3" that a separate "verifier' entity can use when applying hash functions according a special type of technique (called Diffie Helhnan algorithm), this algorithm actually involves the generation of key values by both participants (a "claimant" as shown implementing steps Aa- Ad, Ca-Ce and "verifier" as shown implementing steps Ba-Bfin the paragraph bridging columns 4 and 5)

The prior art references of record do not teach or render obvious the limitations as recited in independent claims 1, 7, 14 and 18 specific to providing a public key comprising an exponent-interval description including said first random limit, and an interval width specification and a public key value derived from the random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret keg, said exponent interval, and two public values from a set of elements having a square root modulo n, such that the random secret key and a selected exponent value from the plurality of exponent elements in said exponent interval ! are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT

Friday, October 24, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436